Department of the Army
United States Army Intelligence Center
and Fort Huachuca
Fort Huachuca, Arizona 85613-6000

***FH Regulation 190-1**

2 July 2001

Military Police

INTRUSION DETECTION SYSTEMS

Summary. This revised regulation explains procedures and requirements to efficiently operate and maintain the Fort Huachuca intrusion detection alarms systems which are monitored by the Directorate of Public Safety.

Applicability. This regulation applies to all elements of the U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) and to all partner organizations. This regulation does not apply to Sensitive Compartmented Information Facilities (SCIFs).

Supplementation. Supplementation of this regulation is prohibited without prior approval from the proponent.

Suggested improvements. The proponent of this regulation is the Directorate of Public Safety (DPS), USAIC&FH. Users may send comments and suggested improvements on the DA Form 2028 (Recommended Changes to Publications and Blank Forms) through channels to Commander, U.S. Army Intelligence Center and Fort Huachuca, ATTN: ATZS-PSE-IS, Fort Huachuca, AZ 85613-6000.

Availability. This publication is available solely on the Fort Huachuca Homepage at http://huachuca-www-army.mil.

Contents

*This regulation supersedes FH Regulation 190-1, 8 July 1997.

Contents (continued)

1. Purpose.

This regulation provides guidance for the procurement, operation, and maintenance of the Intrusion Detection System (IDS) for all USAIC&FH and partner organizations within the confines of Fort Huachuca.

2. References.

Prescribed and referenced publications and forms are available electronically. Fort Huachuca publications and forms are available at http://huachuca-www.army.mil and higher echelon publications and forms are available at http://www.usapa.army.mil. Required publications and referenced forms are listed in Appendix A.

3. Explanation of abbreviations and terms.

Abbreviations and terms used in this regulation are explained in the glossary.

4. Responsibilities.

a. All USAIC&FH directorates, staff offices and partner organizations with IDS will maintain their systems in accordance with (IAW) this regulation.

b. DPS Physical Security will monitor and oversee the operation of IDS IAW this regulation.

c. The Directorate of Engineering and Housing (DEH) will install electrical conduits for IDSs and provide copies of wiring blueprints to Intelligence Electronic Warfare (IEW) Maintenance on all facilities except SCIFs. If the facility is used to process classified material, then the wiring blueprints will be protected IAW AR 380-5.

d. All contractors will be required to follow all guidelines specified in the Corps of Engineers Guide Specifications (CEGS) 16725, Intrusion Detection Systems and DCID 1/21 if the facility is a SCIF. Upon completion of the project, the contractor will submit all diagrams and schematics to DEH and IEW Maintenance unless the facility is a SCIF. If the facility is a SCIF, the schematics will be maintained at the Special Security Office (SSO).

e. IEW Maintenance, 304th Military Intelligence (MI) Battalion (304th MI Bn), 111th MI Brigade will provide maintenance of all IDSs which are not covered by warranty or maintenance contracts. IEW will ensure that all service technicians are qualified as set forth in subparagraphs 6b(1) and (2) of this regulation.

5. General.

The IDS is designed to integrate both defensive and detection measures to protect assets through delay and detection of aggressors.

a. Layers of defense, surrounding the assets, delay aggressors from reaching them. The amount of delay is based on the time it takes to make a 96-square-inch ("mansized") opening in a protected area using a given set of tools once the aggressor has been detected.

b. The IDS sensors should be placed as far as feasible from the asset to detect aggressors before they gain access into the protected areas. In some cases, loud alarms at the sensor location deter aggressors from any further efforts to force entry, but this is not a predictable reaction for all aggressors.

c. The combination of defensive and detection measures must provide maximum defense for the response force to either intercept the aggressor before the asset is compromised or before the aggressor escapes, whichever is preferred. Where the area around the asset is occupied 24 hours a day, an IDS may not be required.

6. Operation, inspections, and tests.

a. All IDS (except reserve units off Fort Huachuca) monitored by the DPS use radio-transmitted alarm signals. Users requiring the installation of an IDS must also consider the appropriate interface and radio equipment. (See paragraph 10.) Contact Physical Security for more information.

b. Personnel.

(1) All Department of Defense or contractor installers, maintenance personnel, and operators of the IDS must be appropriately cleared and undergo a command-oriented security check as described in AR 190-11, paragraph 3-6h(5), prior to being given clearance to arms, ammunition, and explosives (AA&E) facilities or duties and every 3 years thereafter. Other facilities should conduct a command-oriented security check on installers, maintenance personnel, and operators of the IDS.

(2) IEW maintenance technicians must have extensive verifiable work experience with IDSs, Joint-Service Interior Intrusion Detection System (J-SIIDS), as well as some commercial systems and the radio frequency transmitting system being used on Fort Huachuca, prior to hiring.

(3) Agencies using IDS are responsible for training their personnel in the proper operation of their system.

c. Key control. Organizations with AA&E will safeguard and control all keys for IDS, as a minimum, as prescribed in AR 190-11, paragraph 3-8. Other facilities will safeguard and control all keys, as a minimum, as prescribed in AR 190-51, Appendix D.

d. Inspections and tests of the IDS.

(1) As a minimum, organizations with an IDS will thoroughly test the entire system at least quarterly and following any maintenance work to ensure the system is fully operational. There are two exceptions to the quarterly testing; they are Army Reserve units not located on Fort Huachuca and SCIFs. Army Reserve IDSs will be tested monthly IAW U.S. Army Reserve Command (USARC) Pam 190-1. SCIF alarms will be tested IAW DCID 1/21.

(2) Personnel testing the alarms will test each sensor to ensure that the alarm activates. These tests will be recorded on a memorandum and maintained on file at the activity until the next scheduled physical security inspection.

(3) IEW technical maintenance personnel will inspect IDS at intervals not to exceed 6 months to repair or replace worn or failing parts and to detect any indications of possible tampering.

(4) Organizations will conduct the SCIF response tests only after coordination has been made between the DPS Special Security Office (SSO) and the DPS Physical Security Office.

e. Statement of verification. All newly installed IDSs must be certified by the DEH and IEW, on DA Form 4604-R (Security Construction Statement), to ensure that the system meets required standards. All SCIIEs will be certified IAW DCID 1/21 standards. The using agency will maintain this statement on file for future inspections.

f. Access rosters.

(1) DPS Physical Security will provide a listing of all maintenance technicians authorized to work on the IDS. The alarmed area operator (control unit operator) and agency must verify maintenance personnel access by personnel recognition or by identification check. Persons not on this list will not be allowed to work on IDS without special authorization from DPS.

(2) Agencies with alarmed areas will provide DPS with unaccompanied access rosters. The rosters will be verified by the DPS Physical Security Section prior to posting in the alarm monitors station. The rosters will contain the following information on “cleared” personnel (control unit operators), designated to open and close protected areas:

(a) Full name.

(b) Rank.

(c) Social security number and date of birth.

(d) Home and duty phone number.

(e) Duress codes. See definition in section II (Terms) of the Glossary. Using organizations will be responsible for devising and providing duress codes to DPS. These codes must be changed when a person transfers, is removed from the access roster, when compromised, and/or at least every 6 months.

(3) Access rosters will be hand carried to the DPS Physical Security Office, in a sealed envelope, by someone on the access roster to the protected area. Normal processing time is 1 working day upon receipt.

g. IDS failure. In the event of total IDS failure at the alarm monitor station because of computer problems, fire, or natural disaster, etc., the Military Police (MP) will inform alarmed area users of the situation. The MP will make periodic checks of controlled areas as mission dictates; however, alarmed area users will be responsible for taking appropriate action to protect their areas. Controlled areas (SCIFs, vaults, ammunition supply point, and arms rooms) will have guards posted as appropriate.

h. Control unit operator. There are at least two personnel involved with the operations of an IDS: one at the control unit (alarmed area) and the other at the monitoring point in the MP Station. The control unit operator is an individual designated to check the interior of an IDS-protected area, activate the system, and secure the facility. When securing the protected area, the control unit operator will -

(1) Ensure all persons have left the protected area.

(2) Secure all doors and windows except the exit door.

(3) Turn off all lights not required.

(4) Advise the IDS monitor by telephone the area is being closed. State the alarm number and your name to the IDS monitor. After the IDS monitor verifies the information with the access roster, the control unit operator will be allowed to place the control unit into the night or secure position and immediately leave the area and lock the exit door.

(5) Call the IDS monitor back from outside the alarmed area and verify that the system has secured properly. If the facility does not have a telephone outside of the alarmed area, the operator should proceed to a telephone and contact the alarms room monitor to ensure that the system is secure.

(6) Repeat steps 1-5 above if the IDS did not set up in the secure or night position. If the alarm system still will not set up in concert with the IDS monitor, the system will be turned back to access. The operator will also ensure the following is accomplished, if applicable:

(a) A guard will be required to be posted in AA&E storage areas. The arming of this guard is based upon regulatory requirements/local threat condition and the commander’s discretion.

(b) All other activities will be responsible for the security of their own areas and should check their areas during non-duty hours utilizing contract or unit guards until the IDS can be repaired. If contract guards are utilized, it will be at the activity's expense. For SCIFs and SSO the Facility Security Officer will determine guard requirements, as appropriate. The MPs will provide periodic checks of those activities as operational requirements allow.

(c) On the following duty day, the control unit operator will call in a work order for the IDS repair to IEW Maintenance, 304th MI BN, and will follow up the call by submitting a DA Form 2407 (Maintenance Request) for repair of the IDS.

i. IDS monitors. The IDS monitors will be trained in the operation of the computer monitor prior to operating the monitor. Operating procedures will be in accordance with established written procedures.

j. Opening the protected areas. When opening the protected area, the control unit operator will -

(1) Advise the IDS monitor by telephone the alarmed area is being opened prior to opening the area. The control unit operator will state his/her name and the alarm number. After verification by the IDS monitor, access the protected area.

(2) Enter the protected area and immediately place the control unit to the day or access position.

7. Threat.

The semi-skilled intruder is the primary threat to U.S. Army assets. This type of intruder can be expected to attack the locks, doors, windows, vents, walls, floors, and ceilings. The intruder may attempt to stay within an activity during closing or attempt armed robbery by confronting persons on duty. The IDS equipment is designed to detect the semi-skilled intruder who may work individually or as a member of a group when attempting entry without sophisticated equipment or detailed planning.

8. Vulnerabilities.

a. Doors (a primary point of intrusion): An intruder will attempt entry by cutting or breaking the lock and opening the door or by breaking through the door.

b. Walls, ceilings, and floors: An intruder can break through almost any type wall, ceiling, or floor in a matter of seconds or minutes with readily available tools.

c. Windows: Windows, like doors, are a primary point of intrusion and are the hardest to protect.

d. Apertures. An opening of 96-square inches (minimum dimensions of 6 by 16 inches) or larger in walls, ceilings, floors, or doors of a building must be considered as a possible point of entry.

e. Personnel. Personnel are often ready targets for persons bent upon robbery and may be used by an intruder to gain access. For this reason, the MP recommend alarmed areas do not post the name and telephone number of points of contact on the outside of the alarmed area. The names should be provided to the MP Operations Section (ATZS-PSE-O) for inclusion in the MP building security computer system.

9. Maintenance of System.

a. DIS is responsible for maintenance of Government-owned and leased systems to include maintaining blueprints of wiring and devices to include complete IDS layout and termination points. DIS will establish commercial maintenance contracts for the IDSs for which maintenance support is required.

b. IDS service technicians will –

(1) Respond to inspect and repair alarmed area malfunctions during the next working day.

(2) Coordinate with DPS Physical Security if malfunction cannot be corrected or to determine priority if more than one area is malfunctioning.

(3) Check with DPS Physical Security and the alarm monitor to determine the exact nature of the problem.

(4) Inform the MP Operations, DPS Physical Security, and the user of any malfunctions that cannot be resolved with 24 hours and the estimated resolve date.

(5) Make written or verbal recommendations to improve the IDS to the user and DPS Physical Security if appropriate.

c. The IDS monitor will –

(1) Determine if the malfunction is a nuisance alarm or an equipment failure. (Nuisance alarms are defined as an alarm that goes off occasionally for no apparent reason and resets.) The user must physically check the alarmed area at least twice (inside) before silencing the alarm. It is important a thorough check of the protected area be accomplished. An intruder in the area may sometime cause the alarm to appear to be a nuisance alarm.

(2) Inform the user he or she must call in a service order on the next duty day if the problem cannot be resolved or that alarm cannot be reset.

d. Log nuisance and equipment malfunctions on DA Form 2407 and pass on any unusual problems noted to the next relief operator. The day shift operator will brief Physical Security and IEW maintenance personnel of problem areas.

e. Using agency (control unit operator) will -

(1) Attempt to correct nuisance alarms by ensuring alarmed doors or windows are fully closed or by resetting the control box.

(2) Turn the alarm system to access and initiate appropriate security measures (arms rooms must be guarded) if the problem cannot be resolved by the above measures.

(3) Ensure a service order is called in to IEW.

(4) Report abnormal alarm conditions to the IDS monitor and will not tamper with the IDS.

10. Procurement and system design.

a. The U.S. Army Troop Command (ATCOM) funds the procurement and installation of approved commercial IDSs. Programming for these funds is done annually through funding forecasts originated by ATCOM. Early anticipation of requirements and inclusion in funding forecasts may eliminate the necessity for users to fund the purchase and installation of IDSs to include radio interface equipment.

b. Agencies requiring a civilian IDS must obtain permission from the installation major army command prior to purchase and forward with requests all technical data on the system and why it is required over the J-SIIDS, IAW AR 190-13, paragraph 4-7. This information will, as a minimum, be marked “For Official Use Only.”

c. J-SIIDS can be procured at minimal cost to the user as a first time issue from ATCOM. Therefore all requests must be forwarded through DPS Physical Security. DPS will prioritize the installation of the IDS for Fort Huachuca. DEH will provide a listing quarterly to the DPS, ATTN: ATZS-PSE-IS, and to IEW, ATTN: ATZS-LOM-E, of IDS alarm system requests.

d. Regardless of which type of funding is used during procurement, the system MUST include a radio interface unit. In the event that the system does not have the radio interface unit, the IDS will have to be monitored by a civilian agency at the users cost.

e. All IDSs will be procured IAW AR 190-13, Chapter 4 and the Installation Physical Security Plan, Annex I.

f. The IDS must be inspected and a complete operational test performed by a Physical Security Inspector prior to the acceptance of the system. This will be recorded on DA Form 4604-R IAW AR 190-11.

g. Any organization that procures a commercial JDSs will provide copies of service, parts, and warranty manuals for the IDS to IEW maintenance.

h. Contractors who install IDSs which require special test equipment, will provide test equipment for the Physical Security Office and IEW maintenance. The specialized test equipment will then become the property of the U.S. Army.

ABCD-EFG-HJ (MARKS#)
XX XXX 2001

MEMORANDUM FOR Commander, U.S. Army Intelligence Center and Fort Huachuca,
ATTN: ATZS-PSE-IS, Fort Huachuca, AZ 85613-6000

SUBJECT: Personnel Authorized to Access (unit/activity and type facility), ALARM #000.

1. The following named individuals are authorized to open/close alarm #000, building #00000:

RANK NAME	SSN	DOB	DUTY PHONE

2. In the event of an alarm or emergency after hours of operation, the following named individuals should be called:

RANK NAME	SSN	DOB	HOME PHONE

3. Duress Code: Note, five letters or less.

4. The point of contact is the undersigned at extension 0-0000.

SIGNATURE BLOCK

Figure 1. Sample access roster.

Appendix A References

Section I
Required Publications

AR 190-11
Physical Security of Arms, Ammunition, and Explosives

AR 190-13
The Army Physical Security Program

AR 380-5
Information Systems Security

Corps of Engineers Guide Specifications for Military Construction (CEGS) 16725
Intrusion Detection Systems

Director of Central Intelligence Directive (DCID) 1/21
Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)

(The above two publications can be obtained from the SSO and DEH.)

FH Reg 190-11
Installation Physical Security Plan

USARC Pam 190-1
Physical Security Program

Section II
Referenced Forms

DA Form 4604-R
Security Construction Statement

DA Form 2407
Maintenance Request

Glossary

ATCOM
U.S. Army Troop Command

DPS
Directorate of Public Safety

IAW
In accordance with

IDS
Intrusion Detection System

IEW
Intelligence electronic Warfare

DEH
Directorate of Engineering and Housing

MP
Military Police

SCIF
Sensitive Compartmented Information Facility

SSO
Special Security Office

USAIC&FH
U.S. Army Intelligence Center and Fort Huachuca

USARC
U.S. Army Reserve Command

Section II
Terms

Duress codes
A code which personnel on duty transmit as a signal to the alarm monitoring station from which an armed response force can be dispatched if a holdup or a duress situation occurs.

Control unit operator
An individual designated to check the interior of an IDS-protected area, activate the system, and lock up at the end of normal duty hours.

IDS monitor
The person in the MP Station who is monitoring all IDS on the radio-transmitted alarm monitoring system.

Nuisance alarms
An alarm that goes off occasionally for no apparent reason and resets.

(ATZS-IMO-IP)

US ARMY INTELLIGENCE CENTER AND FORT HUACHUCA
OFFICIAL PUBLICATION

OFFICIAL:
JOHN D. THOMAS, JR.
Major General, USA
Commanding

CALVERT T. SINGER
Major, Military Intelligence
Director of Information Management

DISTRIBUTION:
E